IRREDUCIBLE LINEAR HOMOGENEOUS GROUPS WHOSE ORDERS ARE POWERS OF A PRIME*

BY

WILLIAM BENJAMIN FITE

The purpose of this article is to determine as far as possible the connection between the degree of an irreducible linear homogeneous group and its abstract group properties. The discussion will be limited for the most part to groups whose orders are powers of a prime. As a particular phase of the general subject there arises the question as to the circumstances under which a group can be simply isomorphic with irreducible groups of different degrees. The simple group of order 168, for example, is simply isomorphic with irreducible groups of degrees 3, 6, 7, and 8 respectively. On the other hand, I know of no group whose order is a power of a prime that is simply isomorphic with irreducible groups of different degrees. In fact, the following discussion shows that in certain irreducible groups the degree is uniquely fixed by certain abstract properties of the group; and if the degree is not thus uniquely fixed the order of the group must be greater than the seventh power of a prime.

THEOREM I. *A linear homogeneous group G, of class*† k, *all of whose invariant operations are similarity substitutions either is irreducible or is simply isomorphic with each of its irreducible components.*

If G is reducible, suppose that it has been put into its completely reduced form. The invariant operations will not be affected by this change. If in any operation the identity of any irreducible component were associated with a non-identical operation in the other variables, this operation would be non-invariant in G, and would therefore give at least one non-identical commutator. This commutator would also be non-invariant, and none of its successive commutators, except identity, could be invariant. But this is impossible since G is of class k. Hence every irreducible component of G is simply isomorphic with G.

THEOREM II. *A linear homogeneous group G, of order a power of a prime, that has a cyclic central either is irreducible or is simply isomorphic with at least one of its irreducible components.*

* Presented to the Society at the New Haven summer meeting September 3, 1906. Received for publication October 22, 1906.

† Cf. Transactions of the American Mathematical Society, vol. 3 (1902), p. 348.

If G is reducible, suppose that it has been put into its completely reduced form. Then at least one of its irreducible components has at least as many invariant operations as G. If G_1 be such a component, it can easily be shown that G_1 and G are simply isomorphic.

Let G be any group of finite order g that has a cyclic central (distinct from identity). It is simply isomorphic with a regular permutation group, which can be written as a linear homogeneous group. We can therefore think of G as a linear homogeneous group. The coefficients in this group are either zero or unity. The central H of G is generated by an operation h of order a and of the form (when written as a permutation)

$$(x_{1,1}x_{1,2}\cdots x_{1,a})(x_{2,1}x_{2,2}\cdots x_{2,a})\cdots(x_{g/a,1}x_{g/a,2}\cdots x_{g/a,a}).$$

The operation S,

$$y_{i,j}=\sum_{k=1}^{a}\omega^{(k-1)(j-1)}x_{i,k}\quad(i=1,2,\cdots,g/a;\ j=1,2,\cdots,a),$$

where ω is a primitive ath root of unity, transforms G into a semi-canonical form,* and in particular transforms h into its normal form. It is furthermore obvious that the roots of the characteristic equation of h are the ath roots of unity each occurring g/a times.† In the transformed form of G the variables

$$x_{1,j},\ x_{2,j},\ \cdots,\ x_{g/a,j}\qquad(j=1,2,\cdots,a)$$

are transformed into linear combinations of themselves. Let G_j be the group formed by the substitutions of G as far as they affect these g/a variables. If $j-1$ is relatively prime to a, G_j is simply isomorphic with G and its invariant operations are similarity substitutions. If we suppose that G is of class k, it follows from theorem I that G_j is simply isomorphic with each of its irreducible components. Any irreducible component of any G_j $(j=1,2,\cdots,a)$ is an irreducible representation of G. Moreover the components of no two of these G_j's are equivalent. This follows from the fact that in the simple isomorphisms between these components and G the multipliers of the operations that correspond to h are different. We have then $\phi(a)$ distinct irreducible representations of G that are simply isomorphic with it.

It follows directly from this discussion that a sufficient condition that a group of class k be simply isomorphic with an irreducible group is that its central be cyclic.‡

* BLICHFELDT, Transactions of the American Mathematical Society, vol. 5 (1904), p. 313.

† This conclusion is obviously independent of the fact that h is invariant in G. Hence if any regular permutation of order a is written as a linear homogeneous substitution the roots of its characteristic equation are the ath roots of unity, each occurring g/a times, where g is the degree of the permutation.

‡ Cf. Transactions of the American Mathematical Society, vol. 7 (1906), p. 65. The proof given above is much the simpler one.

If now G is an irreducible linear homogeneous group of order p^m (p a prime) and has p^α invariant operations, there are at least $p^{\alpha-1}(p-1)$ distinct irreducible representations of G that are simply isomorphic with it.

Consider the formula *

$$\sum_{i=1}^{r} \chi_k^i \chi_{k'}^i = \frac{p^m}{h_k}.$$

If we let k refer to the conjugate set formed by an invariant operation of order p, then $h_k = 1$, and we have

$$\sum_{i=1}^{s} x_i p^{2n_i} + p^{m-1} = p^m,$$

where x_i is the number of irreducible representations of G of degree p^{n_i} with which G is simply isomorphic, and $\sum_{i=1}^{s} x_i$ is the total number of the irreducible representations with which G is simply isomorphic. If we denote by $\bar{H}$ the subgroup composed of the invariant operations of order p, then, inasmuch as every invariant subgroup of G contains $\bar{H}$, the terms following $x_s p^{2n_s}$ in the left member of the last equation give $\sum \chi_k^j \chi_{k'}^j$ for the group $G/\bar{H}$, where k refers to the conjugate set composed of identity, and therefore the sum of these terms is p^{m-1}.

It follows from what we have seen that $x_i \geqq p^{\alpha-1}(p-1)(i = 1, 2, \cdots, s)$. If one of the irreducible representations with which G is simply isomorphic is of degree † $p^{(m-\alpha)/2}$, then $s = 1$ and $x_1 = p^{\alpha-1}(p-1)$. Moreover, $\sum_{i=1}^{s} x_i$ is the difference between the number of conjugate sets of G and of $G/\bar{H}$. Now this difference is $(p-1)$ times the number of conjugate sets of $G/\bar{H}$ whose operations correspond to operations of G that give no invariant commutators besides identity. Also if every non-invariant operation of G gives an invariant commutator besides identity the degree of G is ‡ $p^{(m-\alpha)/2}$. Hence:

THEOREM III. *A necessary and sufficient condition that an irreducible group of order p^m with p^α invariant operations be of degree $p^{(m-\alpha)/2}$ is that every non-invariant operation give invariant commutators besides identity.*

If G contains a non-invariant operation that gives no invariant commutator besides identity, it must be of degree less than $p^{(m-\alpha)/2}$, and therefore it must contain a non-invariant operation the sum of whose multipliers is not zero.§ Conversely, if G contains a non-invariant operation the sum of whose multipliers is not zero, its degree must be less than $p^{(m-\alpha)/2}$, and therefore it must

* FROBENIUS, Berliner Sitzungsberichte, 1896, II, p. 1363; BURNSIDE, Proceedings of the London Mathematical Society, vol. 33 (1900), p. 153; series 2, vol. 1 (1903), p. 123.

† No one of them can be of greater degree. See Transactions of the American Mathematical Society, vol. 7 (1906), p. 67.

‡ Loc. cit., p. 67.

§ Loc. cit., p. 67.

contain a non-invariant operation that gives no invariant commutator besides identity. It should be remarked that this does not prove that in an irreducible group the sum of the multipliers of a non-invariant operation which gives no invariant commutator besides identity is necessarily different from zero. That is not yet settled.

Suppose that G, of order p^m, is an irreducible group with an abelian subgroup G_δ of index p^δ. Then G contains a subgroup $G_{\delta-1}$ of index $p^{\delta-1}$ that contains G_δ invariantly. None of the irreducible components of $G_{\delta-1}$ can be of degree greater than p. If $G_{\delta-1}$ does not coincide with G it must be invariant in a $G_{\delta-2}$ of index $p^{\delta-2}$. None of the irreducible components of $G_{\delta-2}$ can be of degree greater than * p^2. By proceeding thus with a series of subgroups each of which is invariant in the next following one and of index p under it, we see that the degree of G cannot exceed p^δ.

THEOREM IV. *If an irreducible linear homogeneous group G of order p^m contains an abelian subgroup of order $p^{m-\delta}$, the degree of G cannot exceed p^δ.*

It follows immediately that *if G, of order p^m, has a cyclic central of order p^α and contains an abelian subgroup of order greater than $p^{(m+\alpha)/2}$, it must contain non-invariant operations that give no invariant commutators besides identity.*

If G, of order p^m, is an irreducible group of degree p, it contains an abelian subgroup of order † p^{m-1}. It therefore cannot be simply isomorphic with an irreducible group of any other degree. It can now readily be verified that (as stated in the introduction) if G is of order p^m, where $m < 8$, it cannot be simply isomorphic with irreducible groups of different degrees.

If G_δ is any subgroup of G of index p^δ and with p^{α_1} invariant operations, its degree must be equal to, or less than, $p^{(m-\delta-\alpha_1)/2}$ if it is irreducible, and in case it is reducible the same must be true of each of its irreducible components. If $p^{(m-\alpha-\lambda)/2}$ is the degree of G, then $m+\delta-\alpha_1 \geqq m-\alpha-\lambda$, or $\lambda \geqq \alpha_1-\alpha-\delta$. If we know the degree of G, this inequality gives us an upper limit to the number of invariant operations of any subgroup with a given index. On the other hand, if the abstract group properties of G are known, it gives us an upper limit to the degree of G.

THEOREM V. *If G is an irreducible group of order p^m (p an odd prime) and class 3, the square of the absolute value of the sum of the multipliers of any operation of G is a power of p.*

The theorem is obvious for the invariant operations and for those non-invariant operations the sums of whose multipliers are zero. We need to consider, then, only those non-invariant operations the sums of whose multipliers are not zero.

* This argument is based upon a selection of new variables such as is described by BLICHFELDT, loc. cit., p. 311.

† Transactions of the American Mathematical Society, vol. 7 (1906), p. 68.

Let S be such an operation. Obviously it is not in H_2.* We suppose then that it corresponds to an operation of order p^β of G/H_2. Since S can give no invariant commutator besides identity, there must be in G an operator A such that $S^{-1}AS = At$, where t is commutative with S, but is not invariant in G. Now $S^{-p^\beta}AS^{p^\beta} = At^{p^\beta}$, and therefore t^{p^β} is invariant in G. Moreover $S^{-1}A^{p^\beta}S = A^{p^\beta}t^{p^\beta}h^{[p^\beta(p^\beta-1)]/2}$, where $A^{-1}tA = th$, h being invariant in G. Since t^{p^β} is invariant, $h^{p^\beta} = 1$ and therefore $t^{p^\beta} = 1$, since otherwise S would give an invariant commutator besides identity. If t is of order $p^{\beta_1}(\beta_1 \leqq \beta)$, we put $t_1 \equiv t^{p^{\beta_1-1}}h^{p^{\beta_1-1}(p^{\beta_1-1}-1)/2}$, and $A_1 \equiv A^{p^{\beta_1-1}}$. Then $S^{-1}A_1S = A_1t_1$. Now t_1 is of order p. (If it were identity, $t^{p^{\beta_1-1}}$ would be invariant and therefore $h^{p^{\beta_1-1}} = 1$; but this would require that $t^{p^{\beta_1-1}} = 1$). If $\beta_1 > 1$, A_1 and t_1 are commutative.

Since S and t_1 are commutative, we can consider both of them written in the normal form:

$$S:\quad x_i' = \sigma_i x_i;\qquad t_1:\quad x_i' = \omega_i x_i \qquad (i=1, 2, \cdots, n).$$

Inasmuch as t_1 is not invariant, its multipliers break up into p sets of equals, those of one of the sets being unity. If A_1 and t_1 are commutative, the sum of the multipliers of S that correspond to each of these sets, except that one whose terms are all unity, is zero. If $\beta_1 = 1$ and A is not commutative with t, we shall have:

$$\sigma_i^{-1}\sigma_{p^{n-1}+i}=\omega,\ \sigma_{p^{n-1}+i}^{-1}\sigma_{2p^{n-1}+i}=\omega^2,\ \cdots,\ \sigma_{(p-1)p^{n-1}+i}^{-1}\sigma_i=\omega^p=1 \quad (i=1,2,\cdots,p^{n-1}).$$

From this it follows that

$$\sum_{i=1}^{p^n}\sigma_i = (2+\omega+\omega^3+\cdots+\omega^{[j(j-1)]/2}+\cdots+\omega^{[(p-1)(p-2)]/2})\sum_{i=1}^{p^{n-1}}\sigma_i.$$

If we define χ as the first of the following sums, we have

$$\begin{aligned}
\chi &= 1+\omega+\omega^3+\cdots+\omega^m,\\
\omega^{-1}\chi &= \omega^{-1}+1+\omega^2+\cdots+\omega^{m-1},\\
\omega^{-3}\chi &= \omega^{-3}+\omega^{-2}+1+\omega^3+\cdots+\omega^{m-3},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\\
\omega^{-m}\chi &= \omega^{-m}+\cdots+1,
\end{aligned}$$

where, for brevity, m denotes $p(p-1)/2$.

The sum of the left members of all these equations is $\chi\bar{\chi}$($\bar{\chi}$ being the conjugate imaginary of χ). Therefore, $\chi\bar{\chi} = p + \sigma$, where σ is the sum of the elements of all the columns on the right, except the middle column. Now the sum of the elements of the ith column to the right of the middle one is

* BURNSIDE, *Theory of groups of finite order*, p. 62.

$$\frac{\omega^{i(i+1)/2}\left(1-\omega^{i(p-i)}\right)}{1-\omega^{i}}=\frac{\omega^{i^2/2}-\omega^{-i^2/2}}{\omega^{-i/2}-\omega^{i/2}}.$$

Moreover, the sum of the elements of the ith column from the right end (counting the end one as the first one) is

$$\frac{\omega^{(p-i+1)(p-i)/2}\left(1-\omega^{(p-i)i}\right)}{1-\omega^{p-i}}=\frac{\omega^{i^2/2}-\omega^{-i^2/2}}{\omega^{i/2}-\omega^{-i/2}}.$$

Therefore, the sum of the elements of these two columns is zero. Since there is an even number of columns to the right of the middle one, and since the sum of the elements of any column to the left of the middle one is the conjugate imaginary of the sum of the elements of the corresponding column to the right, we have* $\chi\bar{\chi}=p$. That is, the square of the absolute value of the sum of the multipliers of S is equal to p times the square of the absolute value of the sum of the first p^{n-1} of them.

Consider now the subgroup G_1 of G that is composed of the operations that are commutative with t_1. G_1 is reducible and has p irreducible components. That part of t_1 that belongs to a certain one of these components has all its multipliers equal to unity. In this component either S is invariant or it is a non-invariant operation that gives no invariant commutator besides identity. In the former case the theorem results immediately; in the latter it is necessary to apply the same procedure again. By continuing in this way we must finally come to a component in which S is invariant. Hence the theorem.

The square of the absolute value of the sum of the multipliers of S is at most equal to p^{2n-1}. If we denote by x the number of non-invariant operations of G that give no invariant commutators besides identity, we have $p^{a+2n}+xp^{2n-1}\geqq p^m$; that is, $x\geqq p^{a+1}(p^{m-a-2n}-1)$.

THEOREM VI. *An irreducible group of order p^m (p an odd prime), class 3, and degree $p^{(m-a-\lambda)/2}$ contains at least $p^{a+1}(p^{\lambda}-1)$ non-invariant operations that give no invariant commutators besides identity.*

CORNELL UNIVERSITY,
October, 1906.

* For this evaluation of $\chi\bar{\chi}$ I am indebted to PROFESSOR C. N. HASKINS.